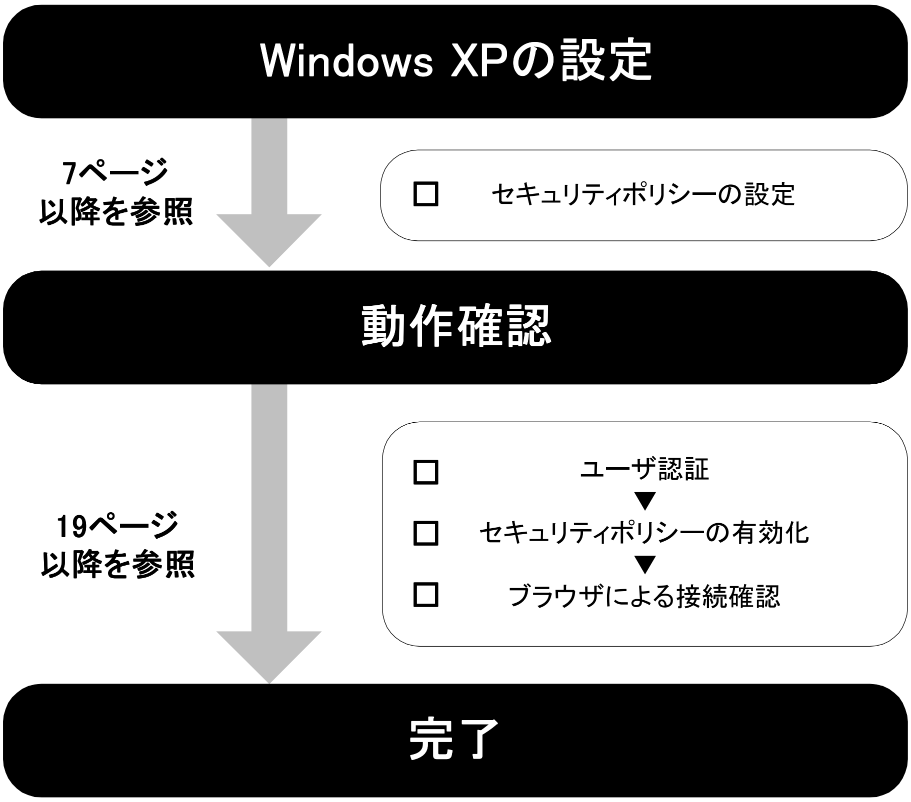
2 VPNクライアントの設定

本章では、Windows XPに標準搭載されているVPNクライアント機能の設定方法について、順番に説明します。

作業の流れ

　Windows XPのVPNクライアント機能を使用してリモートアクセスVPN環境を構築する場合は、図のような流れで作業を行います。



Windows XPの設定

リモートアクセスVPN環境を構築するためには、Windows XP(SG 01)側でセキュリティポリシーを設定しておく必要があります。

セキュリティポリシーの設定

Windows XPにおけるセキュリティポリシーの設定方法について説明します。

ローカルセキュリティ設定の起動

ローカルセキュリティ設定を起動します。

1. [スタート]メニューから[コントロールパネル]→[管理ツール]を選択する。

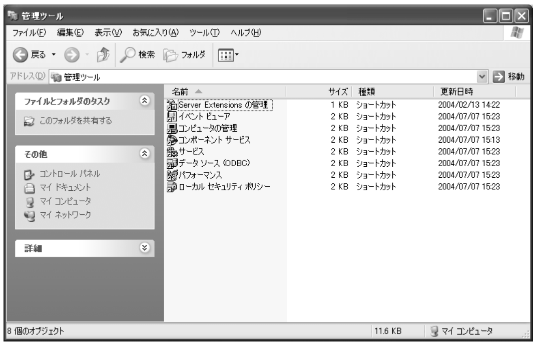
   管理ツール画面が表示されます。

ヒント

コントロールパネル画面が「カテゴリの表示」の場合、[パフォーマンスとメンテナンス]→[管理ツール]を選択します。

2. 「ローカルセキュリティポリシー」をダブルクリックする。

   ローカルセキュリティ設定が起動します。

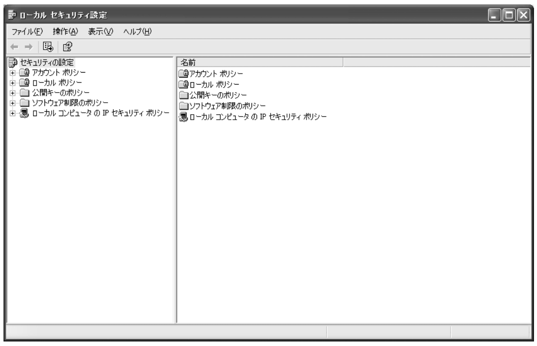


セキュリティポリシーの作成

セキュリティポリシーを新規に作成します。

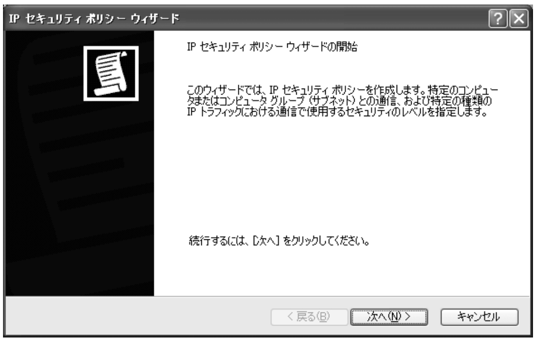
3. 「ローカルコンピュータのIPセキュリティポリシー」を選択し、操作メニューから[IPセキュリティポリシーの作成]を選択する。

   IPセキュリティポリシーウイザードが起動します。



4. ［次へ］をクリックする。

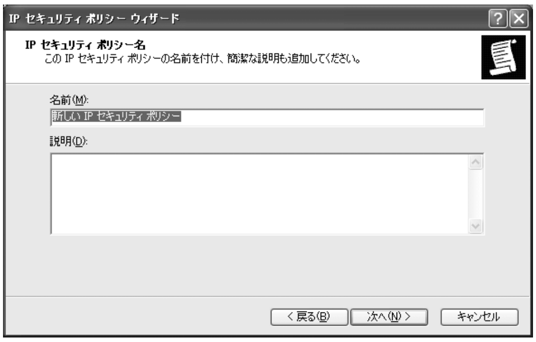
IPセキュリティポリシー名画面が表示されます。



5. 名前の項目に、管理しやすいよう分かりやすい名前を、また、必要に応じて、説明の項目にコメントを入力し、[次へ]をクリックする。

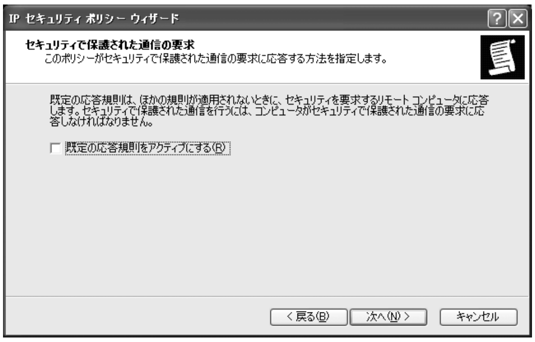
セキュリティで保護された通信の要求画面が表示されます。

（右記の例では名前は「新しいIPセキュリティポリシー」、説明は空白となっています。）



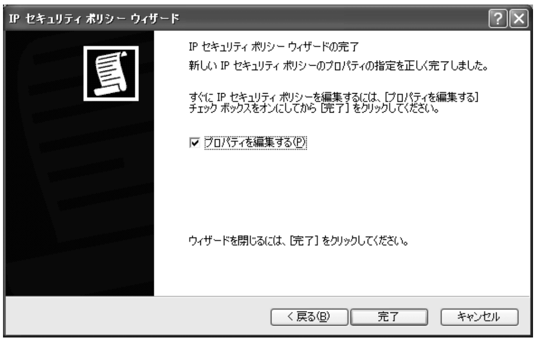
6. 「既定の応答規則をアクティブにする」のチェックを外し、[次へ]をクリックする。

IPセキュリティポリシーウィザードの完了画面が表示されます。



7. 「プロパティを編集する」のチェックボックスのチェックがついているのを確認し、[完了]をクリックする。

新しいIPセキュリティーポリシーのプロパティ画面が起動します。



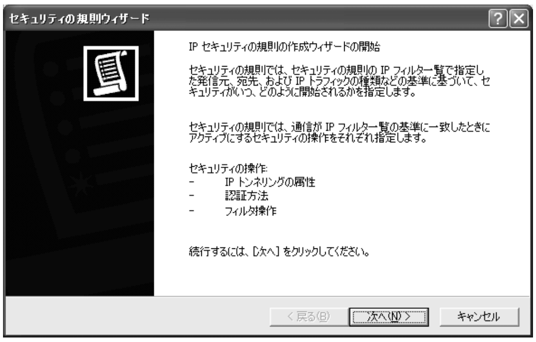
セキュリティ規則の作成

セキュリティ規則を作成します。

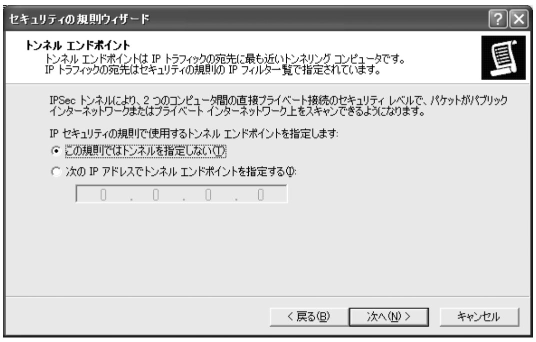
8. [規則]タブをクリックし、[追加]をクリックする。
セキュリティの規則ウィザードが起動し、IPセキュリティの規則のウィザードの開始画面が表示されます。



9. [次へ]をクリックする。
トンネル エンドポイント画面が表示されます。



10. 「この規則ではトンネルを指定しない」のラジオボタンを選択し、[次へ]をクリックする。
ネットワークの種類画面が表示されます。



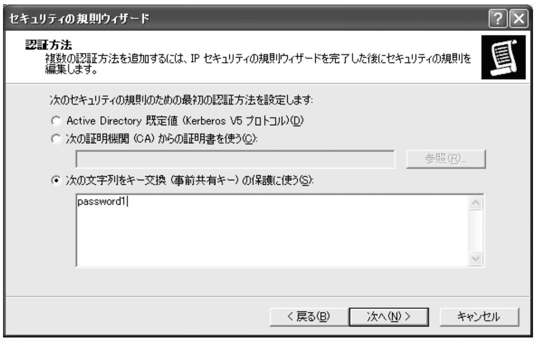
11. 「すべてのネットワーク接続」のラジオボタンを選択し、[次へ]をクリックする。
認証方法画面が表示されます。



１２．「次の文字列をキー交換（事前共有キー）の保護に使う」のラジオボタンを選択し、SG側でVPNパスの設定時に指定したパスワード（プリシェアードシークレット）と同じ鍵の文字列を記し、[次へ]をクリックする。

IPフィルター覧画面が表示されます。

（右記の例では「password1」と記しています。）



鍵の文字列は必ずSG300側でVPNパスの設定時に指定した鍵（パスワード）と同じ文字列を記してください。

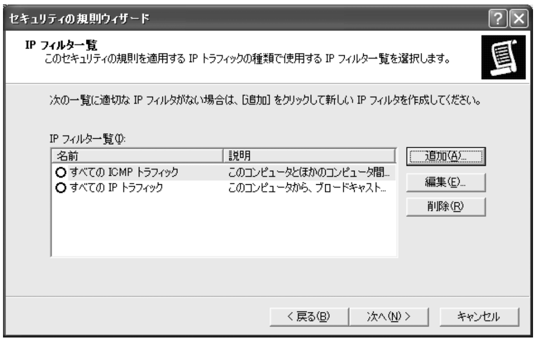
なお、パスワードは必ず英数字を組み合わせて、8文字以上500文字以内で入力します。

●IPフィルタの作成

IPフィルタを新規に作成します。

１３．[追加]をクリックする。

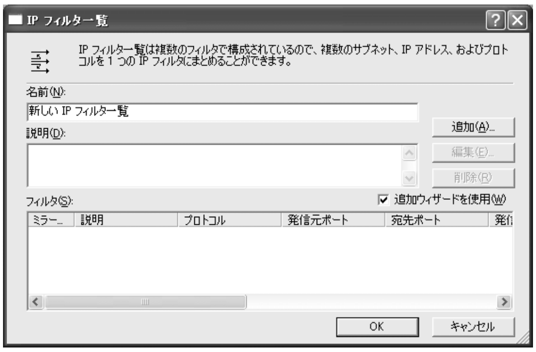
IPフィルター覧が起動します。



１４．名前の項目に、管理しやすいよう分かりやすい名前を、また、必要に応じて、説明の項目にコメントを入力し、[追加]をクリックする。

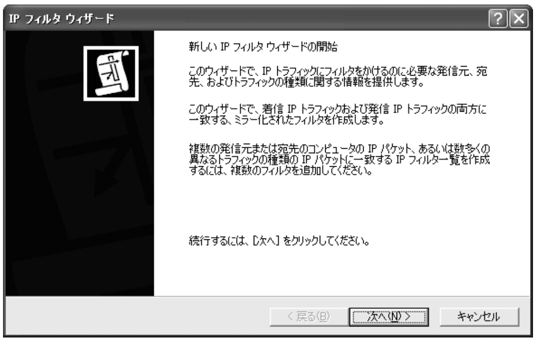
IPフィルタウィザードが起動し、新しいIPフィルタウィザードの開始画面が起動します。

（右記の例では名前は「新しいIPフィルター覧」、説明は空白となっています。）



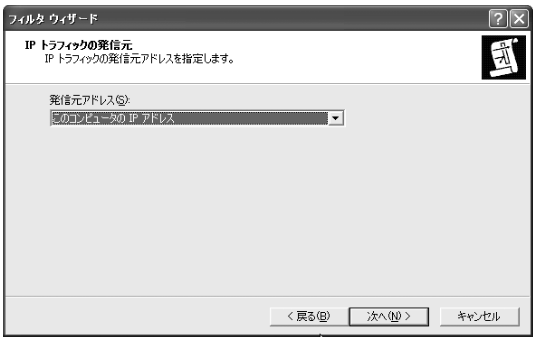
15. [次へ]をクリックする。

IPトラフィックの発信元画面が表示されます。



16. 発信元アドレスのプルダウンメニューから「このコンピュータのIPアドレス」を選択し、[次へ]をクリックする。

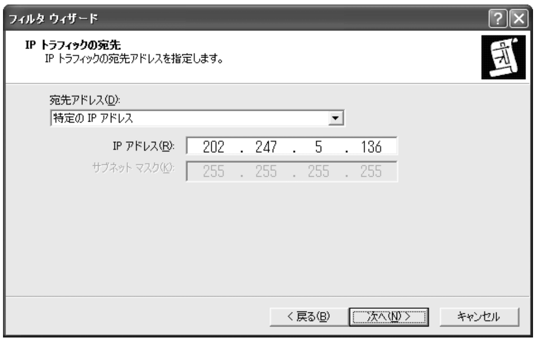
IPトラフィックの宛先画面が表示されます。



17. 宛先アドレスのプルダウンメニューから「特定のIPアドレス」を選択し、IPアドレスには、ファイアウォールのIPアドレスを入力し、[次へ]をクリックする。

IPプロトコルの種類画面が表示されます。

（右記の例では、IPアドレスは「202.247.5.136」となっています。）



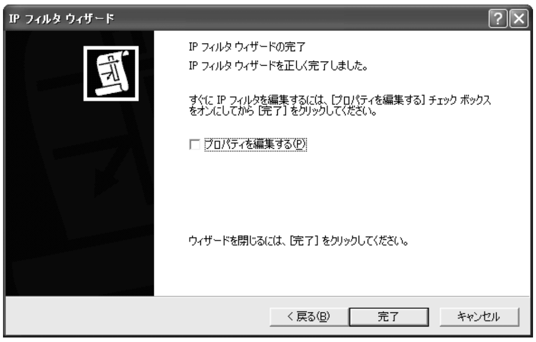
18. プロトコルの種類の選択のプルダウンメニューから「任意」を選択し、[次へ]をクリックする。

IPフィルタウィザードの完了画面が表示されます。



１９．「プロパティを編集する」のチェックボックスのチェックが外れているのを確認し、[完了]をクリックする。

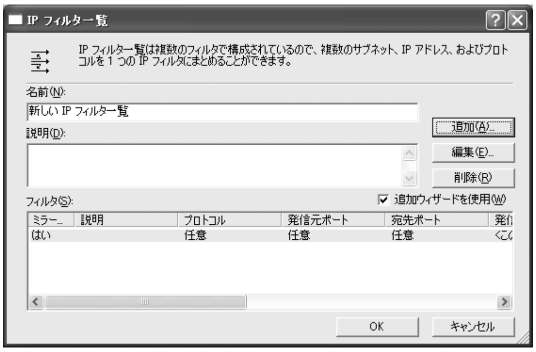
IPフィルター覧画面に戻ります。



２０．フィルタが追加されていることを確認し、[OK]をクリックする。

これでIPフィルタが作成されました。

セキュリティの規則ウィザードに戻ります。



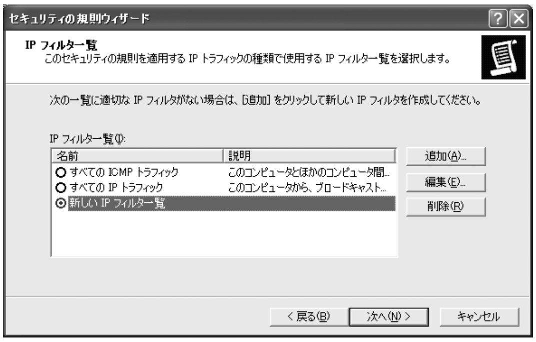
●フィルタ操作の設定

作成したフィルタの操作を設定します。

２１．先に作成したフィルタのラジオボタンを選択し、[次へ]をクリックする。

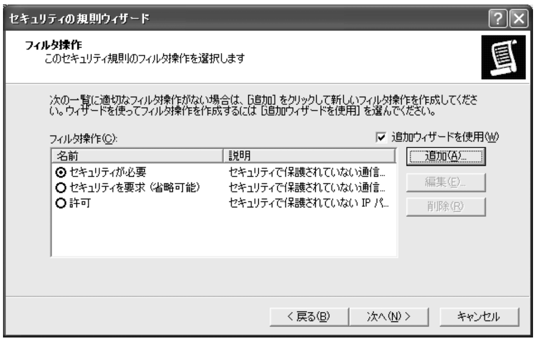
フィルタ操作画面が表示されます。

（右記の例では名前は「新しいIPフィルター覧」となっています。14で入力した名称が記されています。）



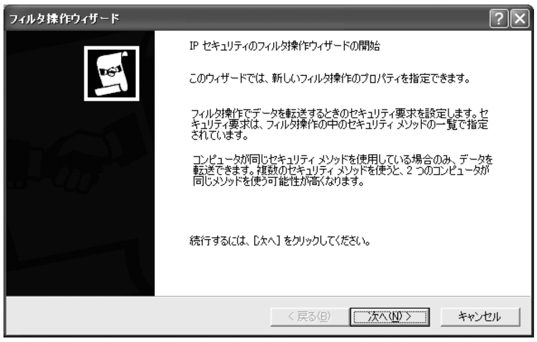
２２．[追加]をクリックする。

フィルタ操作ウィザードが起動し、IPセキュリティのフィルタ操作ウィザードの開始画面が起動します。



23.　[次へ]をクリックする。

フィルタ操作名画面が表示されます。



24.　名前の項目に、管理しやすいよう分かりやすい名前を、また、必要に応じて、説明の項目にコメントを入力し、[次へ]をクリックする。

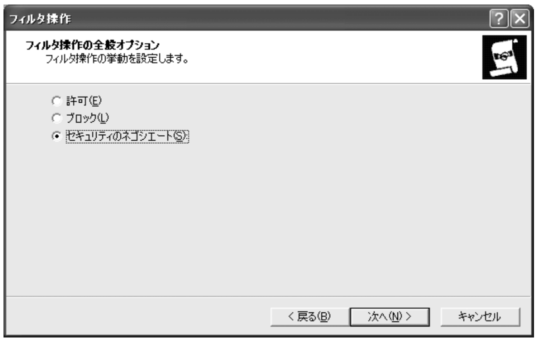
フィルタ操作の全般オプション画面が表示されます。

（右記の例では名前は「新しいフィルタ操作」となっています。）



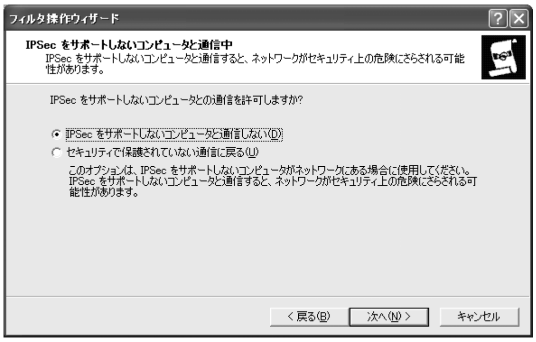
25.　「セキュリティのネゴシエート」のラジオボタンを選択し、[次へ]をクリックする。

IPSecをサポートしないコンピュータと通信中画面が表示されます。



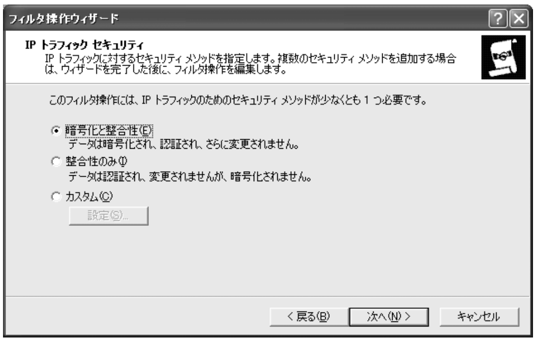
26.　「IPSecをサポートしないコンピュータとは通信しない」のラジオボタンを選択し、[次へ]をクリックする。

IPトラフィックセキュリティ画面が表示されます。



27.　「暗号化と整合性」のラジオボタンを選択し、[次へ]をクリックする。

IPセキュリティフィルタ操作ウィザードの完了画面が表示されます。

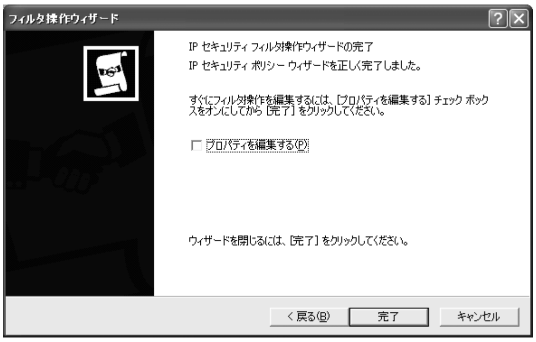


ヒント

IPトラフィックセキュリティ画面では、実際に通信する際に使用する暗号アルゴリズムなどを指定します。

28.　「プロパティを編集する」のチェックボックスのチェックが外れているのを確認し、[完了]をクリックする。

セキュリティの規則ウィザードに戻ります。



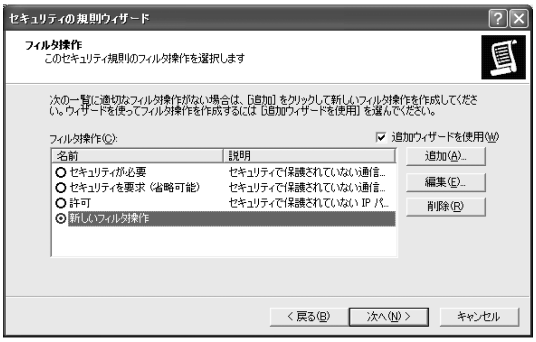
●セキュリティ規則の作成完了

セキュリティ規則の作成を完了します。

29.　先ほど設定したフィルタ操作（24で設定した名前のフィルタ操作）のラジオボタンを選択し、[次へ]をクリックする。

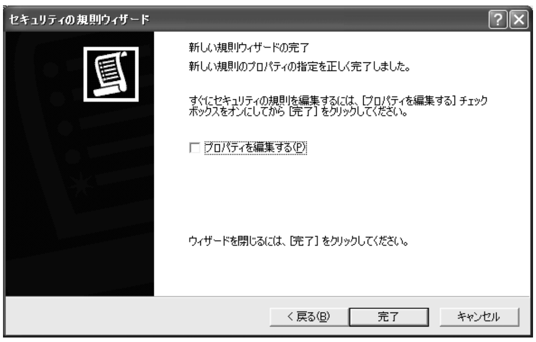
新しい規則ウィザードの完了画面が表示されます。

（右記の例では名前が「新しいフィルタ操作」のラジオボタンを選択します。）



30.　「プロパティを編集する」のチェックボックスのチェックを外し、[完了]をクリックする。

新しいIPセキュリティポリシーのプロパティに戻ります。



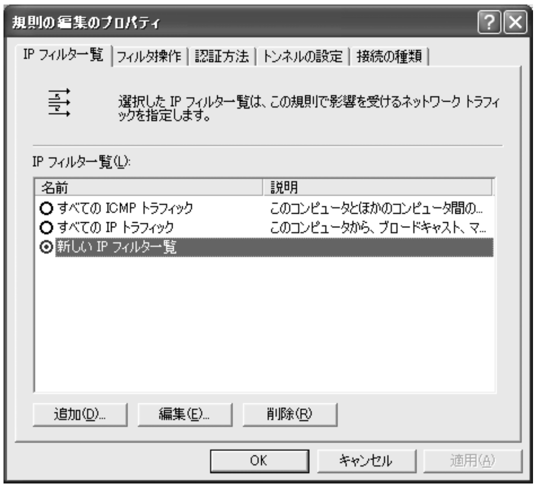
鍵交換の設定

SG300とWindows XP間で行われる鍵交換の際に必要となる項目を設定します。

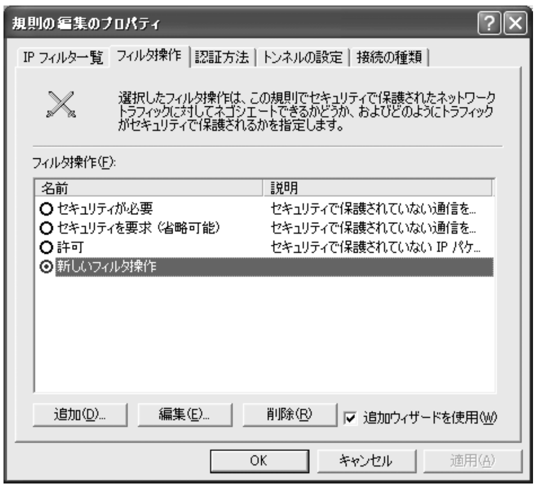
31． IPセキュリティの規則のIPフィルター覧から先ほど設定したフィルタのチェックボックスをチェックし、[編集]をクリックする。
規則の編集のプロパティが起動します。
（右記の例では「新しいIPフィルター覧」をチェックします。）



32． [フィルタ操作]タブをクリックする。



33． 先ほど設定したフィルタ操作（24で設定した名称のフィルタ操作）のラジオボタンを選択し、[編集]をクリックする。
新しいフィルタ操作のプロパティが起動します。
（右記の例では「新しいフィルタ操作」となっています。）



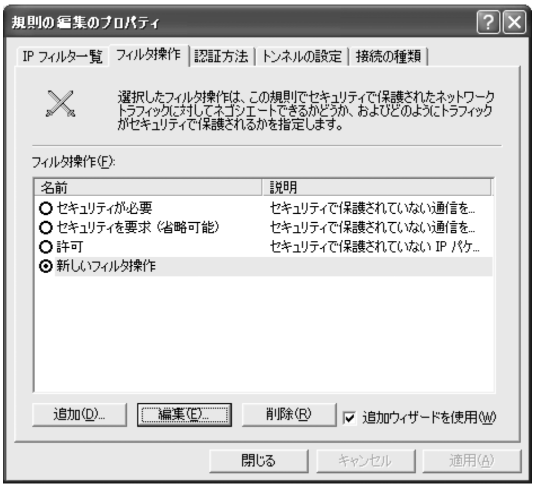
３４． [セキュリティメソッド]タブの「セッションキーのPFS（Perfect Forward Secrecy）」のチェックボックスをチェックし、[OK]をクリックする。

規則の編集のプロパティに戻ります。



３５． [閉じる]をクリックする。

新しいIPセキュリティポリシーのプロパティに戻ります。



３６． [全般]タブをクリックし、「次の設定を使用してキー交換を行う」の[詳細設定]をクリックする。

キー交換の設定が起動します。



３７． 「マスタキーのPFS（Perfect Forward Secrecy）」のチェックボックスをチェックし、「IDの保護に用いるセキュリティメソッド」の[メソッド]をクリックする。

キー交換のセキュリティメソッドが起動します。



ヒント

PFSは、鍵を更新する際、以前の鍵から新しい鍵を推測できないようにする機能です。

３８． 下記のように設定されていることを確認し、[OK]をクリックする。

キー交換の設定画面に戻ります。

種類	暗号化	整合性	Diffie-Hellman
IKE	3DES	SHA1	中（2）
IKE	3DES	MD5	中（2）
IKE	DES	SHA1	低（1）
IKE	DES	MD5	低（1）



３９． [OK]をクリックする。

新しいIPセキュリティポリシーのプロパティに戻ります。



セキュリティポリシーの設定完了

セキュリティポリシーの設定を完了します。

４０． [閉じる]をクリックする。

４１． 以上で、WindowsXPにおけるセキュリティポリシーの設定は完了しました。



動作確認

セキュリティポリシーを設定したWindows XPの動作確認方法について説明します。

●ユーザ認証

●セキュリティポリシーの有効化

●ブラウザによる接続確認

ユーザ認証

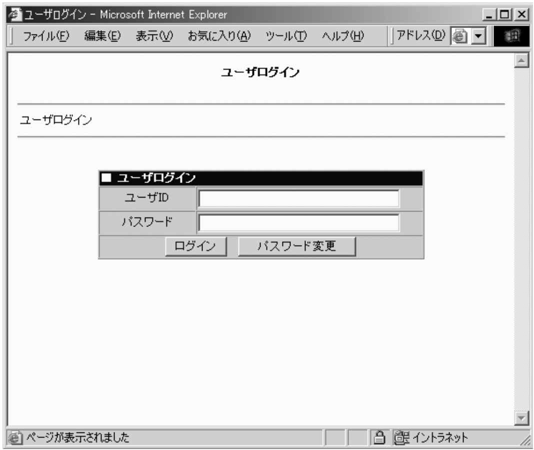
ユーザ認証を行います。

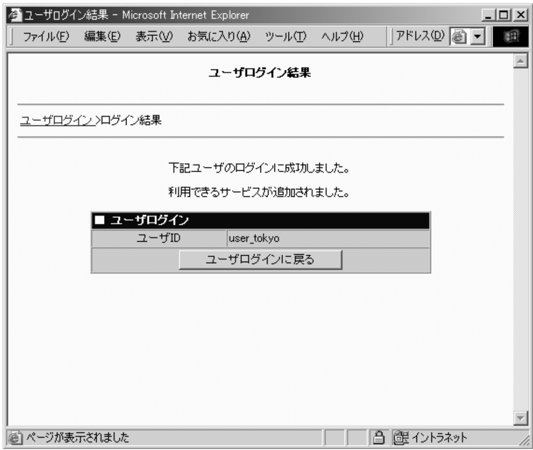
1. Internet Explorer等のブラウザを起動し、SG300側で設定した認証ページ（https://202.247.5.136）にアクセスする。

   ユーザログイン画面が表示されます。

2. SG300側で設定したユーザID（user_tokyo）とパスワードを入力し、[ログイン]をクリックする。

   ログインに成功すると、グループルールで設定したポリシーが追加され、VPNパスが有効になります。





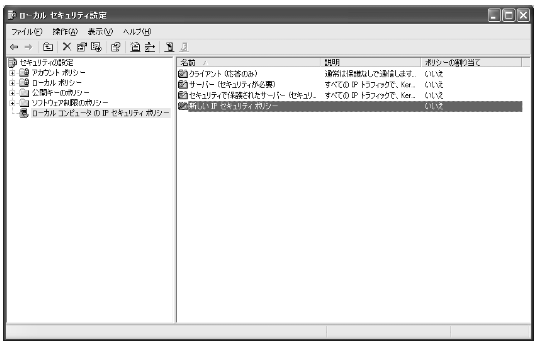
ヒント

SG300側の設定の詳細は、「リモートアクセスVPNの設定（サーバ編）」を参照してください。

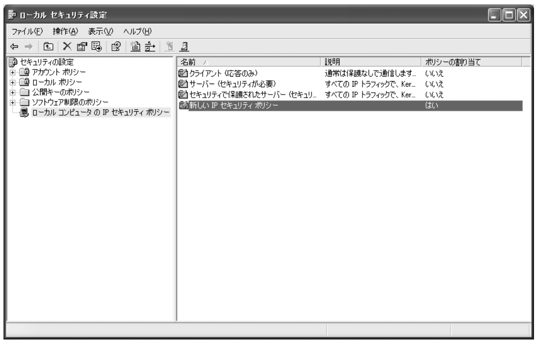
セキュリティポリシーの有効化

設定したセキュリティポリシーを有効にします。

1. ローカルセキュリティ設定を起動し、「セキュリティポリシーの設定」で設定したセキュリティポリシーを選択した後、[操作]メニューから[割り当て]を選択する。（右記の例では「新しいIPセキュリティポリシー」となっています。）



2. ポリシーの割り当ての項目に「はい」と表示されます。選択したセキュリティポリシーが、割り当てられたことを画面上で、確認してください。



3. 以上で、登録したセキュリティポリシーが有効になりました。

ブラウザによる接続確認

SG300とWindows XP間で、VPNによる接続が行えるかどうか確認します。

1. Internet Explorer等のブラウザを起動し、SG300の内側のWebサーバ（http://202.247.5.136/）に接続可能かどうか確認してください。

> ヒント
>
> 接続ができなかった場合は、VPN通信が行われていません。再度、これまでの各設定を見直してください。
>
> 設定を見直しても改善しない場合は、SG300側の設定が正しく行われているか、管理者に確認してください。